IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA *v.* VIKAS SINGLA	Criminal Action No. 1:21-CR-00228-MLB-RDC

United States' Sentencing Memorandum

The United States of America, by Ryan K. Buchanan, United States Attorney, and Samir Kaushal, Assistant United States Attorney for the Northern District of Georgia, and Brian Z. Mund and Lydia Lichlyter, Trial Attorneys of the Department of Justice's Computer Crime and Intellectual Property Section, respectfully files this Sentencing Memorandum in advance of defendant Vikas Singla's sentencing.

Pursuant to the plea agreement, the United States recommends that Singla receive a sentence of 57 months' probation, to include 57 months of home detention. This recommendation is based on Singla's medical condition, which warrants imposition of home detention as an alternative to incarceration to accomplish the specific purpose of permitting Singla to continue his ongoing medical care.

Factual and Procedural Background

Singla is the Chief Operating Officer at Securolytics, a network security business that offers security services to healthcare institutions and other businesses. (Doc. 102-1 at ¶ 12(a).) Securolytics was

struggling financially in the months leading up to Singla's September 2018 cyberattacks on Gwinnett Medical Center ("GMC"). Going approximately a year back from the cyberattack, in October 2017, employee D.B. left Securolytics due to non-payment of wages from approximately August 2017 until October 2017.[1] Contract employee D.M. likewise reported that, around December 2017, Securolytics stopped paying his invoices in full.[2] Employee J.C. similarly reported that Securolytics had a challenging year in 2018 and had funding issues in the September / October 2018 time frame.[3]

In an attempt to generate business for Securolytics, Singla conducted a series of computer intrusions against GMC hospital campuses in Duluth and Lawrenceville, Georgia. (Doc. 102-1 at ¶¶ 12(b), 12(j).) To conduct the cyberattack, Singla began physical reconnaissance of GMC's hospitals on September 22, 2018. (Presentence Investigation Report ("PSR") ¶ 10.) After spending a few

---

[1] (Interview of D.B., filed separately under seal as Exhibit 1, at FBI-000279.)

This sentencing memorandum relies in part on interview memoranda and other information gathered during the investigation. Hearsay is admissible in a sentencing hearing provided it is sufficiently reliable. *United States v. Baptiste*, 935 F.3d 1304, 1315–16 (11th Cir. 2019).

[2] (Interview of D.M., filed separately under seal as Exhibit 2, at FBI-000364.)

[3] (Interview of J.C., filed separately under seal as Exhibit 3, at FBI-000404.)

days learning about GMC, on September 27, 2018, in the middle of the night, at approximately 1:30 am, Singla attacked the ASCOM phone system—a system used by hospital staff to communicate, including for "Code Blue" life-threatening medical emergencies (Doc. 102-1 at ¶ 12(e))—for the GMC Duluth campus. (*See id.* at ¶12(c); PSR ¶ 11.) The attack, which caused the ASCOM phone system to go offline, involved modifying the Unite Connectivity Manager ("UCM") ASCOM configuration file by inserting the text "baidu325061723607132."[4] To access the UCM, Singla inputted without authorization the UCM default password set by the manufacturer.[5] As a result of Singla's modification, over 200 hospital phones at the GMC Duluth hospital were rendered inoperable. (Doc. 102-1 at ¶12(d).)

GMC was unable to fix the hospital phones and enlisted the assistance of ASCOM.[6] With help from ASCOM, GMC attempted to manually reprogram each disabled handset.[7] However, the handsets were once again rendered inoperable around 9 a.m. on September 27,

---

[4](*See* October 31, 2018, email regarding Ascom screenshot and screenshot, filed separately under seal as Exhibit 4, at GMC00000575–76); October 12, 2018, Gwinnett Hospital: Incident Fact Sheet, filed separately under seal as Exhibit 5, at FBI-000916.)

[5] (Ex. 5 at FBI-000916; Interview of B.F., filed separately under seal as Exhibit 6, at FBI-000824; Photo of Unite Connectivity Manager Password Interface, filed separately under seal as Exhibit 7, at GMC00000579.)

[6] (Ex. 5 at FBI-000916.)

[7] (*Id.*)

2018, and the problem was not fully resolved until about five days later, on October 2, 2018.[8]

Singla's cyberattacks were not limited to the ASCOM phone system. At around 4:30 a.m. on the same morning that the ASCOM phones first went down, over 200 network printers across GMC's Duluth and Lawrenceville hospitals, including in the Emergency Departments, began printing out the personally identifiable information of hospital patients, prefaced by the repeated message, "WE OWN YOU!!!"[9] Singla caused the printers to print these threatening messages by sending a file named "Baidu.txt" without authorization. (Doc. 102-1 at ¶12(g).) Singla obtained without authorization the patient data used in the printer attack from a password-protected digitizer connected to a mammogram machine at GMC's Lawrenceville hospital. (*Id.* at ¶¶12(f),(g).) Singla stole the patient information of more than 300 patients from the digitizer. (*Id.* at ¶12(g).)

On October 1, 2018, Singla caused the transmission through the GMC network of over 200,000 unsolicited emails, including about 97,000 emails to email addresses associated with GMC. (PSR ¶ 14.)

---

[8] (*Id.* at FBI-000916–17.)

[9] (Printout Example, filed separately under seal as Exhibit 8, at FBI-000007 (with patient names redacted).)

Singla also caused the transmission of over 300 emails to the email address controlled by the GMC Chief Financial Officer, T.M.[10]

Having sowed fear, uncertainty, and doubt at GMC, Singla began the next phase of his scheme—publicizing the cyberattacks for the purpose of creating marketing fodder that Securolytics could use when offering services to businesses that were concerned for their own safety.[11] (*See* Doc. 102-1 at ¶ 12(j).) On October 2, 2018, again in the middle of the night, from about 2:24 am to 4:45 am, Singla, through a Twitter account with the handle @baidu3250617231[12] and the display name of baidu325061723607132 (the "Baidu Twitter account"), caused the publication of 43 Twitter messages, each of which included the personal identifying information of a different patient.[13] (Doc. 102-1 at ¶¶12(k).) The messages claimed that GMC had been hacked and that the CEO and hospital employees were trying to cover it up. (PSR ¶ 16.) The tweets contained "@" signs for news organizations, like the Gwinnett Daily and the Atlanta Business Chronicle. (*Id.*) The same day

---

[10] (Documentation of Meeting at GMC, filed separately under seal at Exhibit 9, at FBI-000019; Example email to T.M., filed separately under seal as Exhibit 10, at GMC00000063.)

[11] The United States does not contend that Singla personally solicited GMC or personally caused Securolytics to solicit GMC after Singla's cyberattacks.

[12] The factual basis in the plea agreement erroneously omitted the digit "6" from the Twitter handle.

[13] (Twitter Posting Examples, filed separately under seal as Exhibit 11.)

as the tweets, a blog writer contacted the Baidu Twitter account and published a story about the GMC hack. (*Id.*) To further engage the media, the next day, on October 3, 2018, in response to a blog post expressing doubt that GMC had been hacked, Singla, through the Baidu Twitter account, caused the posting of two video captures from cameras within a GMC facility.[14] One image appeared to show an unidentified room with a whiteboard, the other appeared to depict a patient lying in a gurney (later determined to be a training room with a "dummy" patient).[15]

In October 2018, Securolytics used news reporting on Singla's attack against GMC in marketing emails to potential customers.[16]

On June 8, 2021, Singla was charged in an 18-count indictment for his cyberattack on GMC. (Doc. 1.) On November 16, 2023, Singla pleaded guilty to Count One of the Indictment, charging Intentional Damage to a Protected Computer in violation of Title 18, United States Code Sections 1030(a)(5)(A), (b), and (c)(4)(B) and 2. (Doc. 102.)

---

[14] (Ex. 6 at FBI-000824–25; FBI Report of Twitter Posting of Surveillance Camera Image, filed separately under seal as Exhibit 12, at FBI-000811–15.)

[15] (Ex. 12 at FBI-000812.)

[16] (Marketing Email Example, filed separately under seal as Exhibit 13, at SECUROLYTICS-00218750–51.)

Argument

The United States recommends that Singla receive a 57-month term of probation, with all of it to be served on home detention. This recommendation is a significant downward departure in light of how the § 3553(a) factors, including Singla's custody guidelines range, call for a custodial sentence. Notwithstanding the seriousness Singla's conduct, a downward departure of 57 months' probation, with all of it to be served on home detention, appropriately balances the Section 3553(a) factors in light of Singla's medical condition.

1. The nature and circumstances of the offense, the custody guidelines range, and the need for deterrence weigh in favor of a custodial sentence.

Singla's offense conduct was undoubtedly serious. From a Guidelines perspective, his custody guidelines range, which is 57 to 71 months of incarceration, makes that clear. Looking beyond the numbers, though, reveals just how serious this crime was. Singla attacked two hospitals that provide a variety of medical services, including treating newborn infants requiring intensive care in a Neonatal Intensive Care Unit. This was a premeditated campaign aimed at fomenting fear and uncertainty among hospital staff. Singla knowingly disabled the ASCOM phone system used to communicate in the event of life-and-death emergencies. And, with the hospital phones down, he then caused hundreds of printers to print patient names with the threatening message, "WE OWN YOU." He also sent hundreds of

thousands of unsolicited emails, including hundreds to GMC executive leadership.

Singla's cyberattacks, which targeted the sick and vulnerable and those who care for them, were motivated by a desire for money. Singla expected that a high-profile attack on GMC's hospitals would create compelling marketing materials for future Securolytics sales pitches. Determined to publicize that GMC "was #hacked,"[17] Singla publicly exposed the personal information of 43 GMC patients on Twitter in tweets designed to draw interest from the press and cybersecurity experts.[18] Securolytics, when communicating with potential customers, then pointed to the cyberattacks on GMC as a reason to purchase the company's services.[19] Singla's actions, if taken by anyone, would reflect a stunning indifference to how the criminal conduct affected innocent third parties. That Singla is a cybersecurity expert operating in the healthcare space and knew full well the danger to patients and damage to GMC that he was causing makes his criminal acts even more shocking.

The need for adequate deterrence likewise weighs in favor of a custodial sentence. Singla is unlikely to commit further crimes against medical facilities given this criminal case and perhaps a newfound

---

[17] (Ex. 11 at 1.)

[18] (*E.g.*, *id.*)

[19] (Ex. 13.)

appreciation for the importance of healthcare institutions in light of his own condition. As such, specific deterrence may not be a concern here. But general deterrence is crucial here. There is a strong interest in communicating unequivocally to the public that attacks against hospitals, of any kind and for whatever reason, will not be tolerated.

In short, this crime typically would require a custodial sentence.

2. Singla's history and characteristics weigh in favor of a non-custodial sentence.

Singla's personal characteristics distinguish his case from others. Around August 2023, the United States learned that Singla had a stage II diagnosis of a rare and aggressive form of cancer for which there is no available radiation or chemotherapy treatment. Surgical removal of potentially infected portions of the body is the current method of preventing the spread of the cancer. Based on information provided by defense counsel and treating physicians, and the review of relevant scientific literature, the United States determined that, while Singla was currently believed to be cancer-free, his prognosis was extremely poor. For example, based on one published study of 14 patients with Stage II of this rare cancer that received surgery, 12 of those 14 patients died of the disease with a median survival rate of 14.4 months.[20] All patients in the study recurred even with surgery.[21] The

[20] (Indiana University of Medicine Oncology Study, filed separately under seal as Exhibit 14, at 1.)

[21] (*Id.* at 2.)

median recurrence-free survival in that study was 9.8 months and the longest recurrence-free period in the study was approximately 19.63 months.[22] It has now been approximately 16 months since Singla underwent a surgical procedure. (PSR ¶ 61.) The United States also learned that notwithstanding Singla's world-class medical care, effectively removing every cancerous cell would be extremely difficult. And because the only treatment involves surgical removal of infected areas, if Singla's aggressive cancer does return, timely prevention and surgical treatment would be necessary to save Singla's life.

Based on information available in November 2023, the United States agreed that recommending that Singla serve a guidelines-length sentence under home detention for Singla to receive necessary medical care served the interests of justice. The rare, aggressive, and largely incurable and untreatable nature of Singla's cancer diagnosis drives the United States' recommendation. *See* USSG § 5H1.4 ("An extraordinary physical impairment may be a reason to depart downward; e.g., in the case of a seriously infirm defendant, home detention may be as efficient as, and less costly than, imprisonment."); *see also id.* § 5F1.2 (noting that, in appropriate circumstances, home detention may be imposed as a condition of probation as a substitute for imprisonment); *but see United States v. Smith*, 128 F. App'x 89, 90 (11th Cir. 2005) (unpublished) (weakened immune system causing

[22] (*Id.* at 4.)

vulnerability to future illnesses based on cancer in remission insufficient to satisfy Section 5H1.4).[23]

This recommendation should not be misunderstood to suggest that a prior cancer diagnosis or even ongoing cancer treatment would typically render a custodial sentence inappropriate.[24] Each case must be evaluated based on its own facts. *Compare United States v. Sandoval,* No. 94 CR 714-5, 1998 U.S. Dist. LEXIS 9183, 1998 WL 325186, at *6 (N.D. Ill. June 8, 1998) ("Therefore, the court concludes that [defendant's] advanced cancer is an extraordinary physical impairment within the meaning of Section 5H1.4 and warrants a downward departure.") *with Swiss v. United States*, No. CRIM. 1:08CV076, 2008 U.S. Dist. LEXIS 121250, 2008 WL 820269, at *4 (W.D.N.C. Mar. 20, 2008) ("For these reasons the Court cannot find or conclude that Petitioner would be eligible for a downward departure under § 5H1.4 in light of the Petitioner's cancer diagnosis and the treatment available to him through the Bureau of Prisons.").

---

[23] *Smith* is distinguishable from this case because that court found that non-Hodgkin's lymphoma in remission (a less serious diagnosis) was an extraordinary medical condition without considering the probability of a relapse and was focused on the defendant's immunodeficiencies. 128 F. App'x at 90.

[24] Singla's treatment thus far, including his surgical treatment, has given rise to various other medical concerns, including a potentially dangerous vascular condition for which Singla receives medical treatment. These other concerns—without the rare, aggressive cancer diagnosis—do not warrant the downward departure being sought here.

Conclusion

For these reasons, and others that will be presented at sentencing, the United States respectfully recommends that the Court impose a sentence of 57 months' probation, all of which should be served on home detention.

Respectfully submitted,

RYAN K. BUCHANAN
United States Attorney

/s/ SAMIR KAUSHAL
Assistant United States Attorney
Georgia Bar No. 935285
Samir.Kaushal@usdoj.gov

/s/ BRIAN Z. MUND
Trial Attorney, Computer Crime and Intellectual Property Section, Department of Justice
Brian.Mund@usdoj.gov

/s/ LYDIA D. LICHLYTER
Trial Attorney, Computer Crime and Intellectual Property Section, Department of Justice
Lydia.Lichlyter@usdoj.gov